# Improving the anaylsis precision of JavaScript programs via assertion

**Hongki Lee**
Department of Computer Science, KAIST
petitkan@kaist.ac.kr

## MOTIVATION

### SAFE

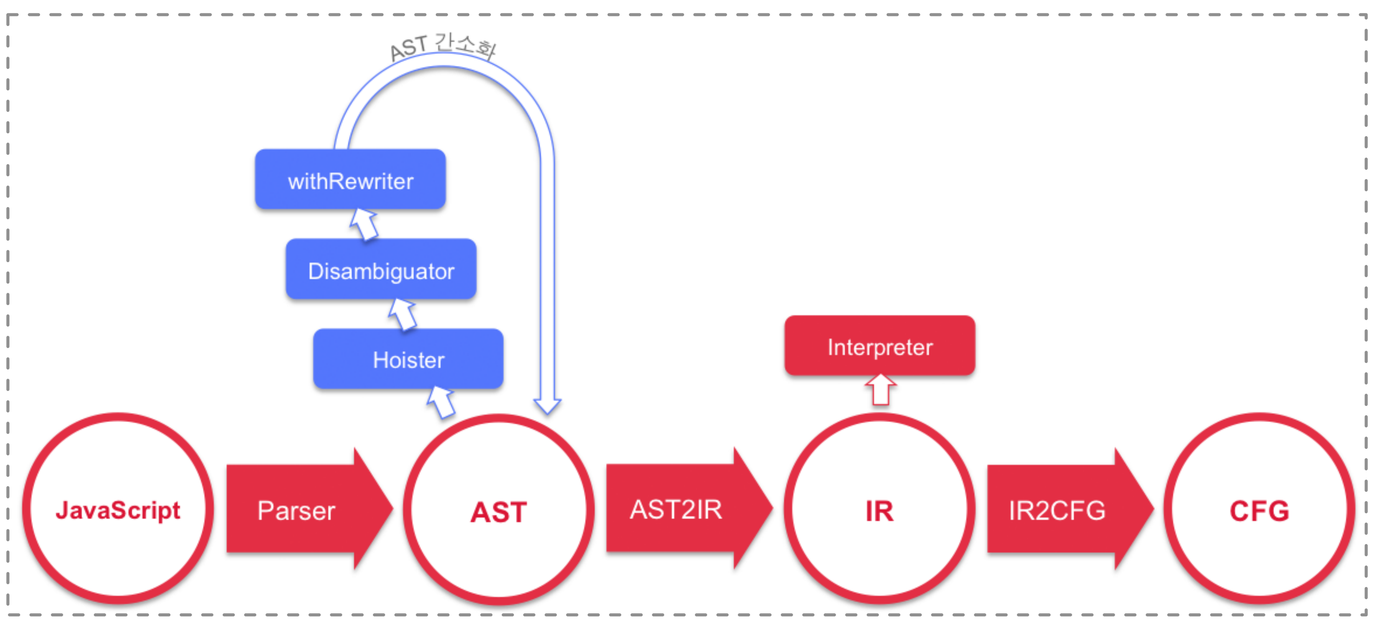
- 기존 도구들의 사용이 불편
- 범용적인 자바스크립트 분석 도구의 필요

### assert

- 자바스크립트의 분석의 정확도 높이기
- 분기노드의 조건을 이용하여 더 나은 분석결과를 얻기

## SAFE

### Big Picture




### Intermediate Representation

| AST | IR | CFG |
|---|---|---|
| 자바스크립트 코드를 표현 | 자바스크립트 프로그램 실행에 편리 | 자바스크립트 프로그램 흐름에 대한 표현 |

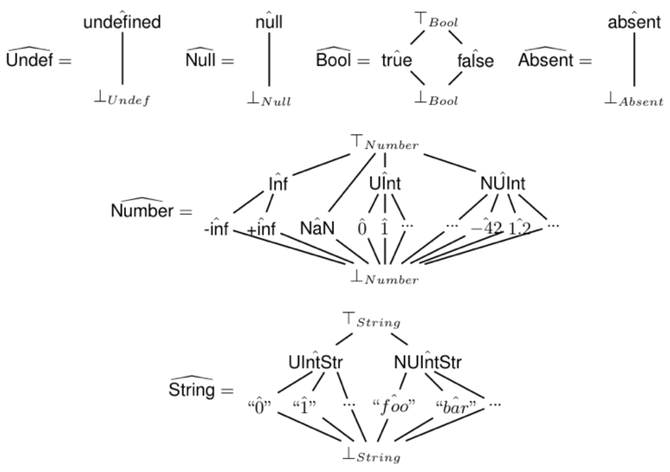
### Translation

**AST2IR**
비슷한 의미를 가지는 노드를 통합

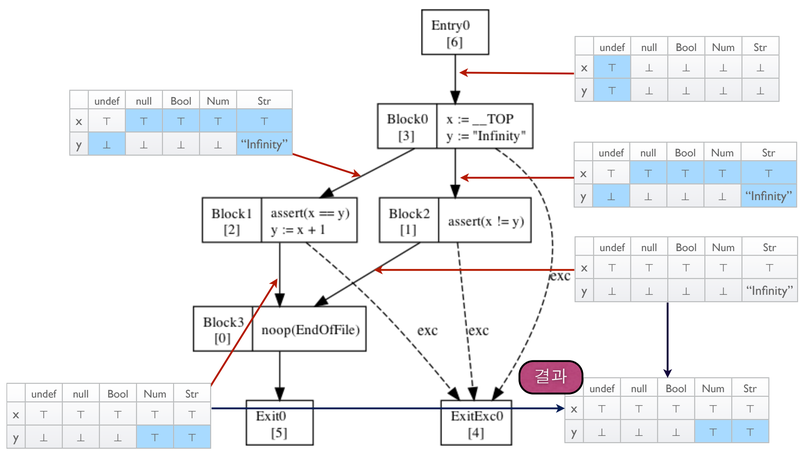
**IR2CFG**
프로그램의 흐름에 맞게 CFG 생성

## assert

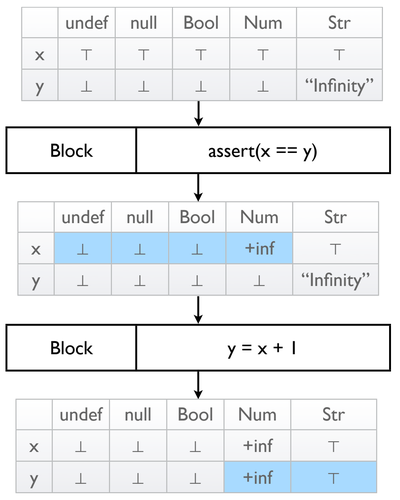
### Abstract Domain




### Baseline Analyzer




### assert on Branches

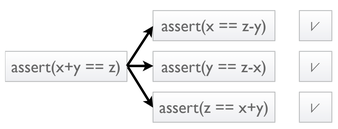



### Branch Processing Mechanism

#### Arithmetic Operators

Initial State

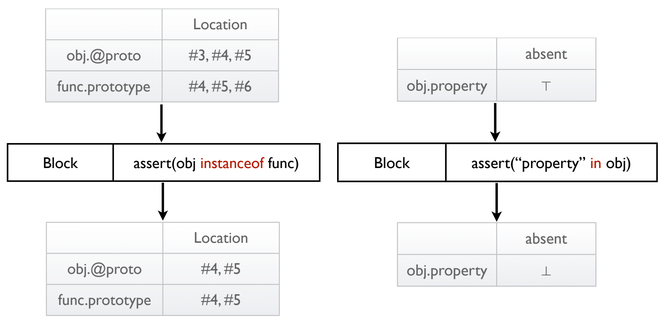
| | undef | null | Bool | Num | Str |
|---|---|---|---|---|---|
| x | ⊥ | ⊥ | ⊤ | UInt | ⊥ |
| y | ⊥ | ⊥ | ⊤ | 2 | ⊥ |
| z | ⊥ | ⊥ | ⊥ | ⊤ | ⊥ |




validity / evaluate & prune

| | undef | null | Bool | Num | Str |
|---|---|---|---|---|---|
| x | ⊥ | ⊥ | ⊤ | UInt | ⊥ |
| y | ⊥ | ⊥ | ⊤ | 2 | ⊥ |
| z | ⊥ | ⊥ | ⊥ | UInt | ⊥ |

#### Object Operators




### Evaluation

(단위:%)

| SunSpider Benchmark | assert문 활용 전 분석 정확도 | | | assert문 활용 후 분석 정확도 | | |
|---|---|---|---|---|---|---|
| | deref | access | type | deref | access | type |
| access-binary-trees | 61.4 | 100 | 86 | 61.4 | 100 | 92(+6) |
| access-nbody | 75.4 | 95.6 | 76.3 | 75.4 | 95.6 | 78.3 (+2) |
| bitops-nsieve-bits | 81.2 | 66.7 | 100 | 100 (+18.8) | 66.7 | 100 |
| date-format-tofte | 93 | 100 | 100 | 100 (+7) | 100 | 100 |
| mat-cordic | 93.3 | 98.6 | 93.3 | 98.7 (+5.4) | 100 (+1.4) | 93.3 |
| math-spectral-norm | 86 | 80.8 | 100 | 92.1 (+6.1) | 80.8 | 100 |

- deref : property access 시 객체부분이 항상 한개의 객체
- access : property access 시 프로퍼티부분이 항상 한개 값
- type : type변환함수의 인자가 가지는 type이 항상 한개

## Limitation

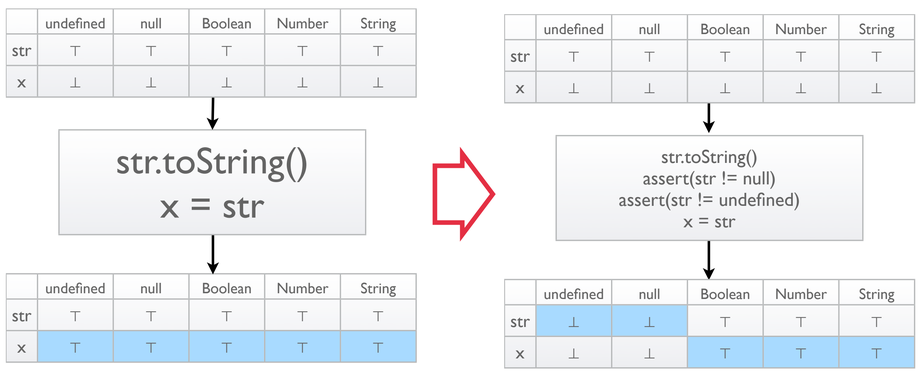
구간 분석이 아닌 단일 값 분석 도메인

➔가능한 산술 연산자의 개수 제한

적극적인 암묵적 타입 변환

➔숫자의 경우, 여러 문자열이 될 수 있음

## Application Plan




자바스크립트 특성에 따라 비 정상 종료 흐름의 값을 제외시킴으로써 더 정확한 값을 얻음